NETWORK ADMINISTRATION & PENETRATION TESTING LAB

Koffivi Joel M. AMETEPE

© Koffivi Joel M. AMETEPE – Tous droits réservés
Ce document est la propriété intellectuelle de son auteur. Toute reproduction, modification, diffusion ou utilisation partielle ou totale sans autorisation écrite est strictement interdite.

SOMMAIRE DU PROJET

1. **Introduction générale**
   1.1. Objectifs pédagogiques du lab
   1.2. Technologies mises en œuvre

2. **Topologie réseau globale**
   2.1. Schéma réseau détaillé
   2.2. Plan d'adressage IP
   2.3. Répartition des rôles

3. **Configuration réseau (Cisco & IP)**
   3.1. Routage OSPF
   3.3. Routage statique (si utilisé)
   3.4. NAT & ACL (sur R4)

4. **Administration système Windows**
   4.1. Configuration du serveur WS2019
   4.2. Installation des rôles (AD, DNS, DHCP, IIS)

5. **Administration système Linux**
   5.1. Installation d'Ubuntu Server
   5.2. Installation de Zabbix
   5.4. Supervision des postes clients

6. **Scans de vulnérabilités internes**
   6.1. Présentation des outils utilisés (Nmap, Nikto, Nessus)
   6.2. Scans de vulnérabilités internes

7. **Bonnes pratiques & documentation**
   8.1. Sauvegarde et snapshots
   8.2. Sécurisation des accès
   8.3. Nommage cohérent
   8.4. Journalisation des actions

8. **Axes d'amélioration**
   9.1. Intégration d'un firewall (pfSense, Cisco ASA, iptables…)
   9.2. Ajout de serveurs web vulnérables (DVWA, Metasploitable)
   9.3. Redondance réseau et haute disponibilité
   9.4. Suggestions de la communauté

Note au lecteur

Ce laboratoire a été conçu pour des utilisateurs ayant déjà une maîtrise de l'installation de machines virtuelles et de l'utilisation de GNS3. Ce document constitue uniquement un **résumé de la mise en place de la topologie et des services du réseau interne**, sans détailler les étapes d'installation de l'environnement ni les configurations de base comme l'installation des OS ou de GNS3.

Il s'adresse donc à des personnes disposant déjà des compétences nécessaires pour préparer l'infrastructure et souhaitant se concentrer sur la configuration avancée du réseau, des services, et la mise en œuvre de la supervision et des tests de sécurité.

1. Introduction Générale

1.1 Objectifs pédagogiques du lab

Ce projet de laboratoire a été conçu comme un environnement immersif , destiné à consolider et à mettre en pratique les compétences clés dans les domaines suivants :

- Réseaux informatiques : compréhension et configuration du routage dynamique (OSPF), des ACL (Listes de Contrôle d'Accès), du NAT et du plan d'adressage IP dans un réseau structuré.
- Administration système : gestion de serveurs Windows (Active Directory, DNS, DHCP,) et de serveurs Linux (supervision avec Zabbix).
- Supervision réseau : implémentation de solutions de monitoring en environnement hétérogène pour observer la disponibilité, les performances et l'état de sécurité des équipements et services.
- Cybersécurité offensive : introduction aux tests de vulnérabilité grâce à la distribution Kali Linux et ses outils intégrés (Nmap, Nikto, Nessus, etc.).
- Ce lab simule un environnement d'entreprise réel, permettant aux apprenants de reproduire des situations techniques courantes : déploiement de services, gestion de réseau multi-sites, détection d'attaques, et surveillance proactive.

1.2 Technologies mises en œuvre

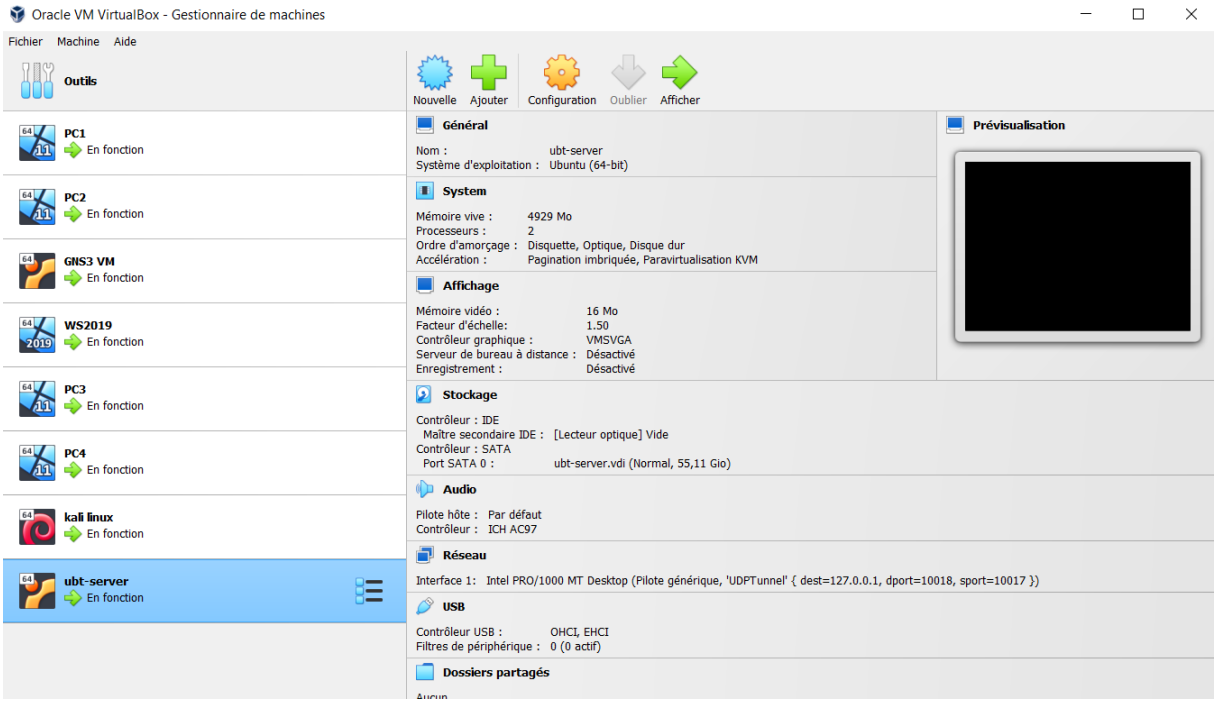
Le lab repose sur une architecture réaliste, intégrant plusieurs technologies et outils professionnels :

- Réseaux Cisco : Configuration de routeurs et switchs via GNS3.
- Virtualisation : Machines virtuelles Windows Server 2019, Ubuntu Server, Kali Linux,Virtualbox
- Protocoles & services : OSPF, NAT, DHCP, DNS, HTTP/HTTPS, ICMP, SNMP.
- Outils de supervision : Zabbix.
- Sécurité offensive (Pentest) : Outils Kali pour audit et tests de vulnérabilité
- Administration de domaine : Contrôleur Active Directory avec gestion centralisée des utilisateurs et des ressources.

Ce lab a été pensé pour être modulaire, scalable et réutilisable dans d'autres contextes pédagogiques ou professionnels.

Il constitue un excellent tremplin vers la certification (Cisco, Linux, Windows Server, CEH, etc.), mais aussi un outil concret pour monter en compétence en environnement d'entreprise.

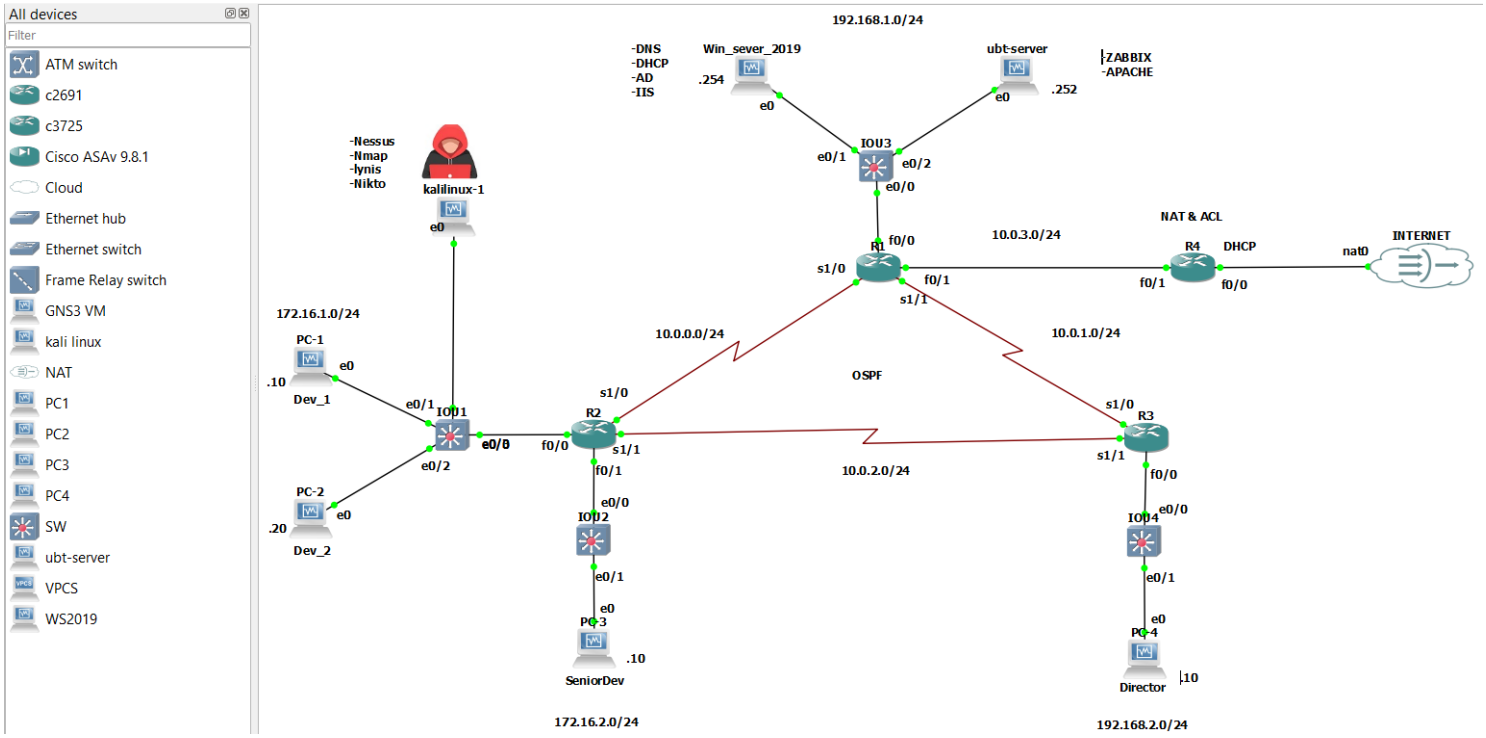
❖ Prérequis pour débuter le lab. :



- installer au moins 4 client windows 11 sur virtualbox (video disponible en dessous)
  https://youtu.be/mPQSqWrIZpY?si=M_15U8DCTctpwptr
- -installer windows server 2022 ou 2019 : (video disponible ci-dessous)
  https://youtu.be/hf0ByiAyn7E?si=CsqsKZ-B2PiS40Sj
- -installer ubuntu server : (video disponible ci-dessous)
  https://youtu.be/36g17uWC1VY?si=sV3knXEbGdZE3JyL
- -installer gns3 et gns3 VM sur virtual box et ajouter les machines :
  https://youtu.be/IQekERpy1-E?si=W-NeRleBra5-qdfh
- -Ajouter les routeurs cisco a Gns3
  https://youtu.be/-IqmDOlsmVY?si=uUGJ-VWlOOzjT55X

2. Topologie Réseau Globale

2.1 Schéma réseau détaillé



Le lab est structuré autour d'un réseau multi-segmenté simulant l'architecture d'une entreprise moderne avec plusieurs départements. Il repose sur quatre routeurs (R1 à R4), chacun desservant un segment du réseau, tous interconnectés via un backbone OSPF. Le réseau est conçu pour :

- Séparer les services et utilisateurs par sous-réseaux.
- Tester les protocoles de routage dynamique.
- Appliquer des politiques de sécurité par des ACL.
- Simuler un accès Internet via NAT.
- Mettre en œuvre une supervision centralisée.

2.2 Plan d'adressage IP

Voici la répartition des sous-réseaux et adresses IP :

Segment réseau	Adresse réseau	Équipements connectés
LAN Dev_1 & Dev_2	172.16.1.0/24	PC-1, PC-2, PC Kali Linux
LAN SenioreDev	172.16.2.0	PC-3
LAN Directeur	192.168.2.0/24	PC-4 (poste du Directeur)
LAN Serveurs	192.168.1.0/24	WS2019-1, ubt-server-1

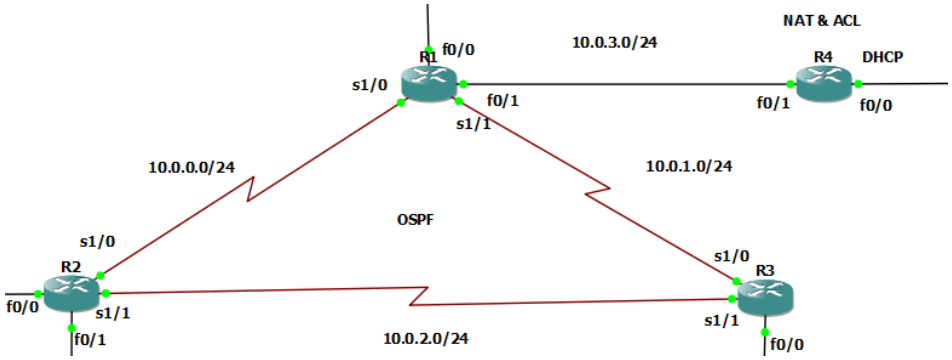
Config interface exemple :

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/1
R1(config-if)#ip add 10.0.3.1 255.255.255.0
R1(config-if)#no sh
```

solarwinds | Solar-PuTTY free tool © 2019-2024 SolarWinds Worldwide, LLC. All righ

Équipement	Interface	Adresse IP	Réseau
R1	f0/0	192.168.1.1	192.168.1.0/24
	s1/0	10.0.0.2	10.0.0.0/24
	s1/1	10.0.1.2	10.0.1.0/24
	s1/0	10.0.3.1	10.0.3.0/24
R2	f0/0	172.16.1.1	172.16.1.0/24
	f0/1	172.16.2.1	172.16.2.0/24
	s1/0	10.0.0.1	10.0.0.0/24
	s1/1	10.0.2.1	10.0.2.0/24
R3	f0/0	192.168.2.1	192.168.2.0/24
	s1/0	10.0.1.1	10.0.1.0/24
	s1/1	10.0.2.2	10.0.2.0/24
	f0/1	10.0.3.1	10.0.3.0/24
R4	f0/0	DHCP	Internet
	f0/1	10.0.3.2	10.0.3.0/24

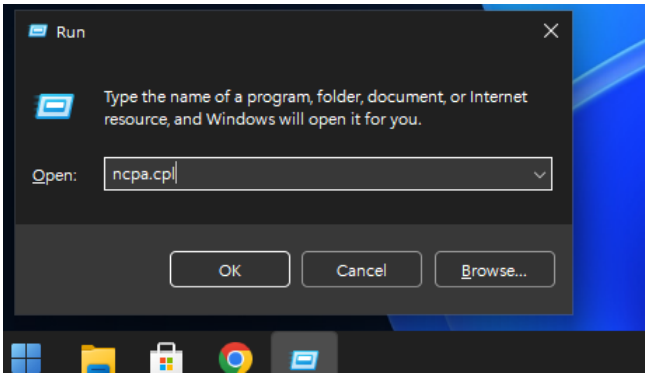
R1 { 10.0.0.0 } R2 R1 { 10.0.1.0 } R3 R2 {10.0.2.0} R3 R4 {10.0.3.0} R4 all= /24



📌 Les plages d'adresses ont été attribuées pour refléter une hiérarchie logique : séparation des services, des postes utilisateurs, et des machines de supervision.

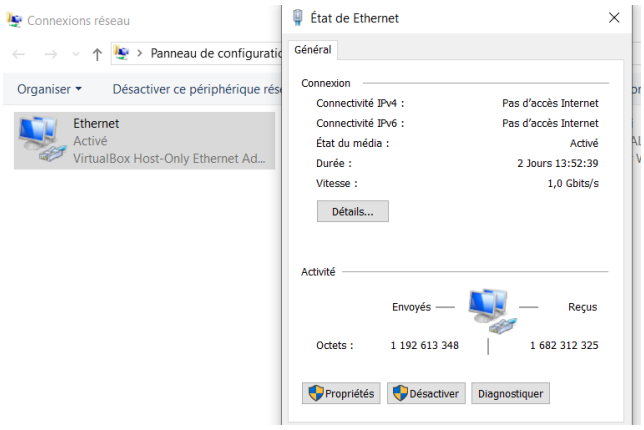
2.3 Répartition des rôles

🖳 Postes Utilisateurs

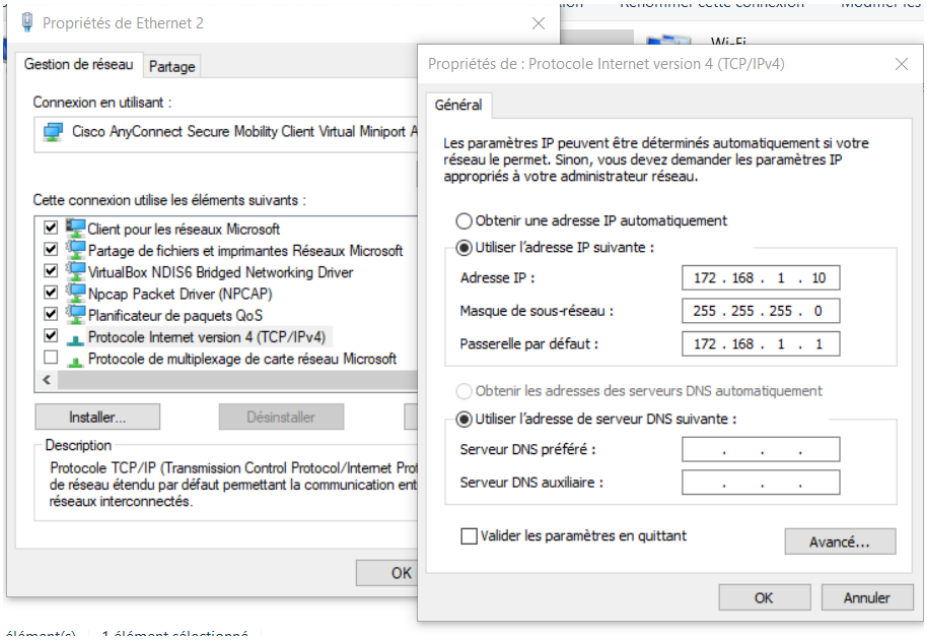


Tapez windows+R et metter la commande ncpa.cpl

Cliquer sur Ethernet puis sur Propriétés



Cliquer sur Ethernet puis sur Propriétés


Propriétés de Ethernet 2
Gestion de réseau
Partage
Connexion en utilisant :
Cisco AnyConnect Secure Mobility Client Virtual Miniport A
Cette connexion utilise les éléments suivants :
Client pour les réseaux Microsoft
Partage de fichiers et imprimantes Réseaux Microsoft
VirtualBox NDIS6 Bridged Networking Driver
Npcap Packet Driver (NPCAP)
Planificateur de paquets QoS
Protocole Internet version 4 (TCP/IPv4)
Protocole de multiplexage de carte réseau Microsoft
Installer...
Désinstaller
Description
Protocole TCP/IP (Transmission Control Protocol/Internet Prot
de réseau étendu par défaut permettant la communication ent
réseaux interconnectés.
OK
Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP :
172 . 168 . 1 . 10
Masque de sous-réseau :
255 . 255 . 255 . 0
Passerelle par défaut :
172 . 168 . 1 . 1
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré :
Serveur DNS auxiliaire :
Valider les paramètres en quittant
Avancé...
OK
Annuler

Machine	IP	Mask	getway	Rôle
PC-1	172.16.1.10	255.255.255.0	172.16.1.1	Développeur
PC-2	172.16.1.20	255.255.255.0	172.16.1.1	Développeur
PC-3	172.16.2.10	255.255.255.0	172.16.2.1	Dev Senior
PC-4	192.168.2.10	255.255.255.0	192.168.2.1	Directeur

Serveurs

Serveur	IP	Services
WS2019-1	192.168.1.254	AD, DNS, DHCP, IIS
ubt-server-1	192.168.1.252	Apache, Zabbix,

Machine de Pentest

Machine	IP (statique ou DHCP)	Outils
Kali Linux	172.16.1.X	Nmap, Nikto, Lynis, Nessus

Cette topologie met en place un environnement riche, modulaire et évolutif, propice aux scénarios d'apprentissage allant de la configuration réseau à la sécurisation et supervision des infrastructures.

3-Configuration Routeur : (tout ce fait dans le mode d'accès privilégier ' conf t ')

R1-R2-R3-R4

######## sécurité de premier niveau #############

enable secret cisco

line console 0

password cisco

login

end

line Vty 0 15

password cisco

login

end

service password-encryption

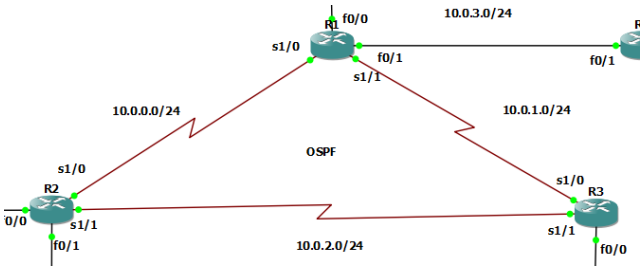
banner motd #enter the password#

do copy running-config startup-config

######## Routage OSPF #######

R 2	R3	R1
router ospf 10	router ospf 10	router ospf 10
router-id 2.2.2.2	router-id 3.3.3.3	router-id 1.1.1.1
network 10.0.0.0 0.0.0.255 area 0	network 10.0.1.0 0.0.0.255 area 0	network 10.0.0.0 0.0.0.255 area 0
network 10.0.2.0 0.0.0.255 area 0	network 10.0.2.0 0.0.0.255 area 0	network 10.0.1.0 0.0.0.255 area 0
network 172.16.1.0 0.0.0.255 area 0	network 192.168.2.0 0.0.0.255	network 192.168.1.0 0.0.0.255 area 0
network 172.16.2.0 0.0.0.255 area 0		

Le protocole OSPF (Open Shortest Path First) a été choisi pour sa stabilité et sa convergence rapide dans les environnements d'entreprise.



@@@@@@@@ ROUTAGE STATIQUE ENTRE R1 ET R4 @@@@@@@@

Ce routage permet une connectivité de tout le réseaux a internet via R4 et met en avant les configuration de protocole NAT et ACL.

R4 # interface f0/0

#ip add dhcp

#no sh

R1# ip route 0.0.0.0 0.0.0.0 10.0.3.2

R4#ip route 10.0.0.0 255.255.255.0 10.0.3.1

#ip route 10.0.1.0 255.255.255.0 10.0.3.1

#ip route 10.0.2.0 255.255.255.0 10.0.3.1

#ip route 172.16.0.0 255.255.0.0 10.0.3.1

#ip route 192.168.2.0 255.255.255.0 10.0.3.1

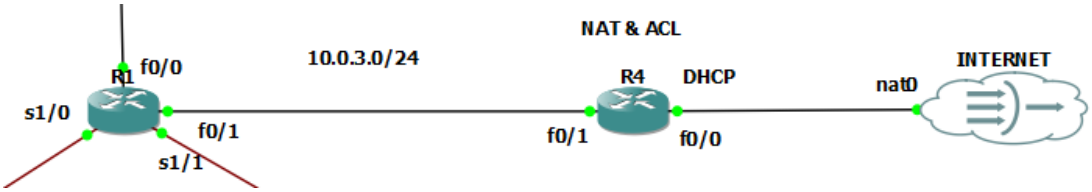
#ip route 192.168.1.0 255.255.255.0 10.0.3.1

#ip route 0.0.0.0 0.0.0.0 192.168.122.1 (vous mettrez l'adresse IPgetway donner par le NAT)

R2# ip route 0.0.0.0 0.0.0.0 10.0.0.2

R3# ip route 0.0.0.0 0.0.0.0 10.0.1.2

Ce routage permet une connectivité de tout le réseaux a internet via R4



NB : les switches n'ont besoin d'aucune config (ils seront utilisés dans le cadre de mise en œuvre VLAN plus tard).

###################### NAT R4 ######################

conf t

! Définir quelles adresses doivent être NATées (ici tout le réseau interne 10.0.0.0/8 par ex)

access-list 1 permit 10.0.0.0 0.255.255.255

access-list 1 permit 172.16.0.0 0.0.255.255

access-list 1 permit 192.168.0.0 0.0.255.255

! Activer le NAT sur l'interface INTERNET (f0/0) comme interface externe

interface f0/0

 ip nat outside

! L'interface côté LAN (f0/1) vers le réseau interne

interface f0/1

 ip nat inside

! Activer le NAT overload pour que toutes les adresses privées partagent l'IP publique de R4 sur le Wi-Fi

ip nat inside source list 1 interface f0/0 overload

4-Administration système Windows

AUTORISER LE DHCP ET LES DNS SUR CHAQUE ROUTEUR POUR ACTIVE DIRECTORY :

**********Sur R2**********

interface f0/0   (! vers LAN 172.16.1.0/24)

 ip helper-address 192.168.1.254

interface e0/0   (! vers LAN 172.16.2.0/24)

 ip helper-address 192.168.1.254

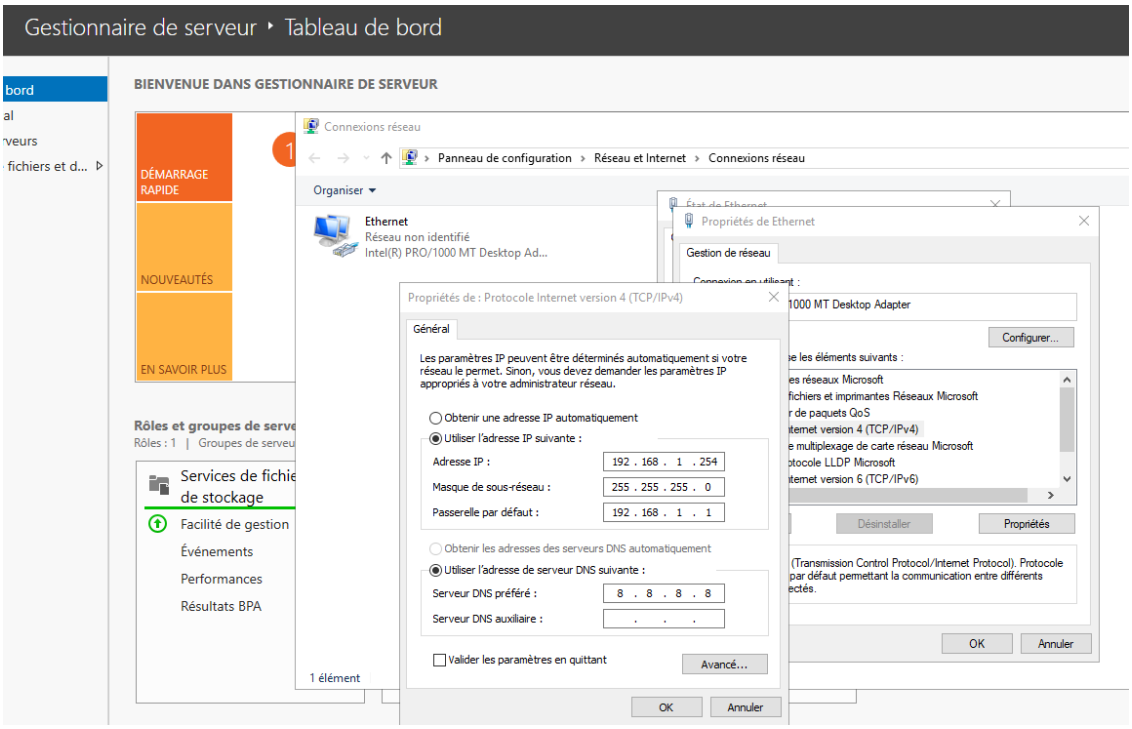
**********Sur R3**********

 interface f0/0   (! vers LAN 192.168.2.0/24)

 ip helper-address 192.168.1.254

4.1. Configuration du serveur WS2019

Attribuons l'adresse 192.168.1.254 à notre serveur Windows :

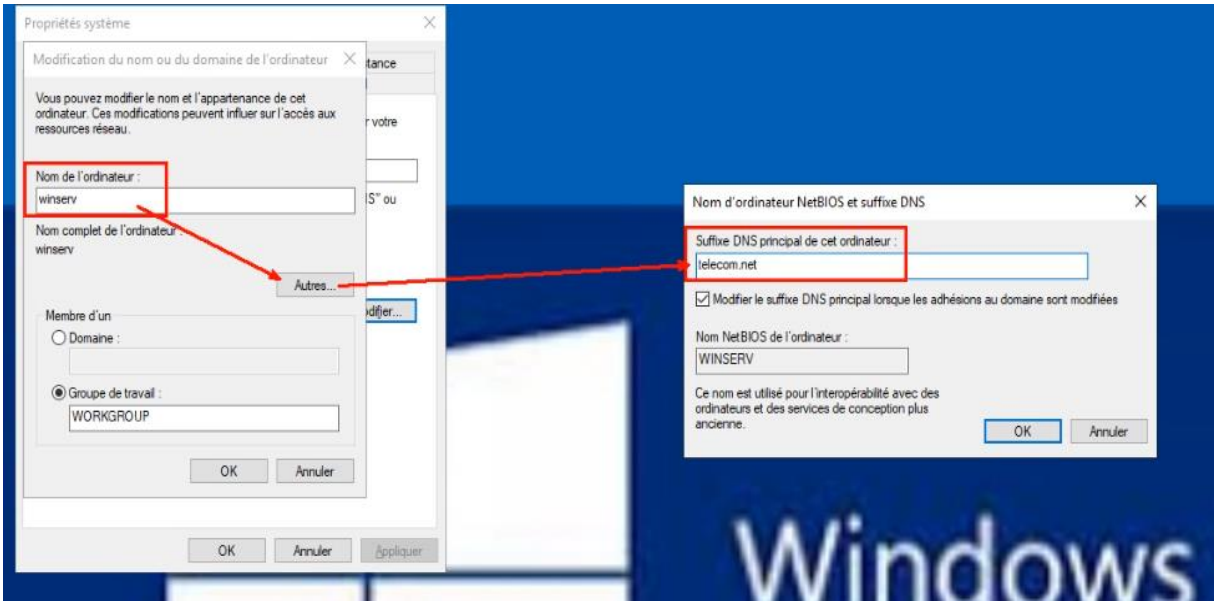

Gestionnaire de serveur • Tableau de bord
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
DÉMARRAGE RAPIDE
NOUVEAUTÉS
EN SAVOIR PLUS
Connexions réseau
Panneau de configuration › Réseau et Internet › Connexions réseau
Organiser
Ethernet
Réseau non identifié
Intel(R) PRO/1000 MT Desktop Ad...
Propriétés de Ethernet
Gestion de réseau
Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 192 . 168 . 1 . 254
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut : 192 . 168 . 1 . 1
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré : 8 . 8 . 8 . 8
Serveur DNS auxiliaire :
Valider les paramètres en quittant
Avancé...
OK
Annuler
Configurer...
Désinstaller
Propriétés
Rôles et groupes de serv
Rôles : 1 | Groupes de serveu
Services de fichi
de stockage
Facilité de gestion
Événements
Performances
Résultats BPA
1 élément

-Tapez Windows + R dans votre serveur et entre la commande sysdm.cpl et cliquer sur modifier.

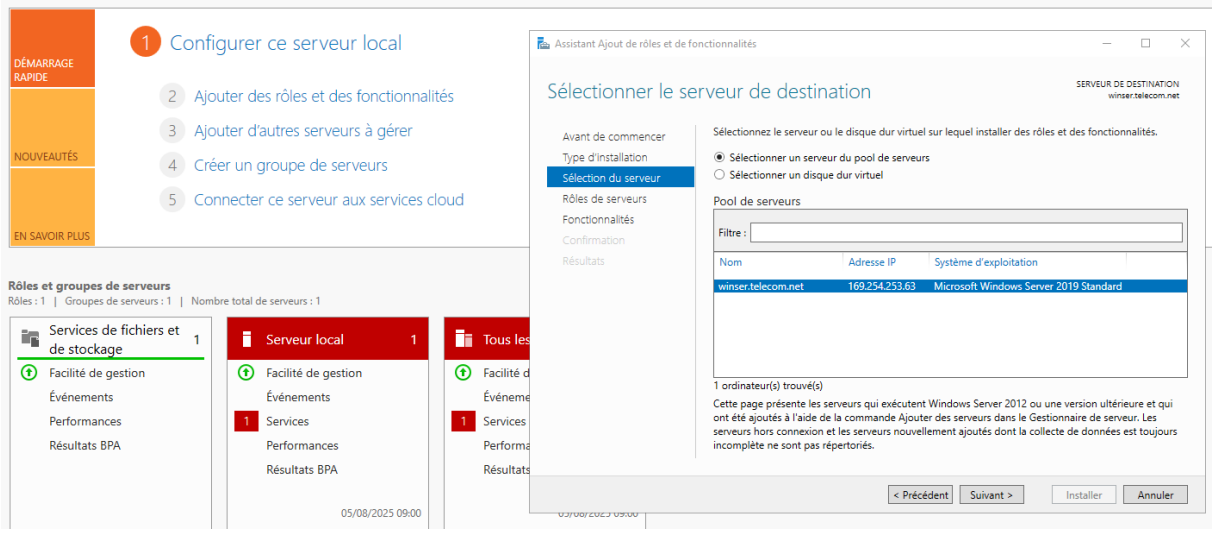
-Modifiez le nom de l'ordinateur dans les propriété système comme suit puis cliquer sur autre et mettez

Nom : Winserv Suffix DNS : telecom.net (autres = sboy.net ou Network.net)

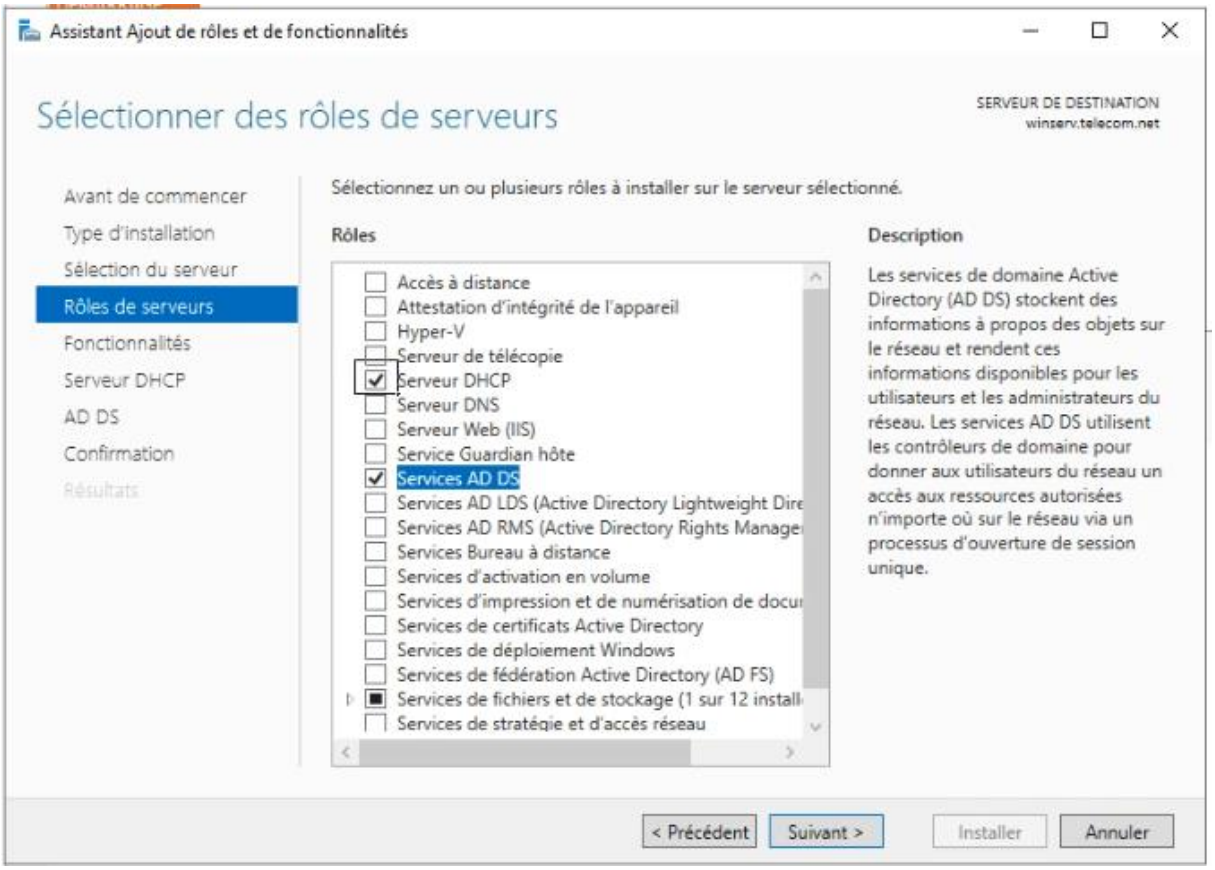
-redémarrer votre machine.


Propriétés système
Modification du nom ou du domaine de l'ordinateur
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.
Nom de l'ordinateur :
winserv
Nom complet de l'ordinateur :
winserv
Autres...
Membre d'un
Domaine :
Groupe de travail :
WORKGROUP
OK
Annuler
Appliquer
Nom d'ordinateur NetBIOS et suffixe DNS
Suffixe DNS principal de cet ordinateur :
telecom.net
Modifier le suffixe DNS principal lorsque les adhésions au domaine sont modifiées
Nom NetBIOS de l'ordinateur :
WINSERV
Ce nom est utilisé pour l'interopérabilité avec des ordinateurs et des services de conception plus ancienne.
Windows

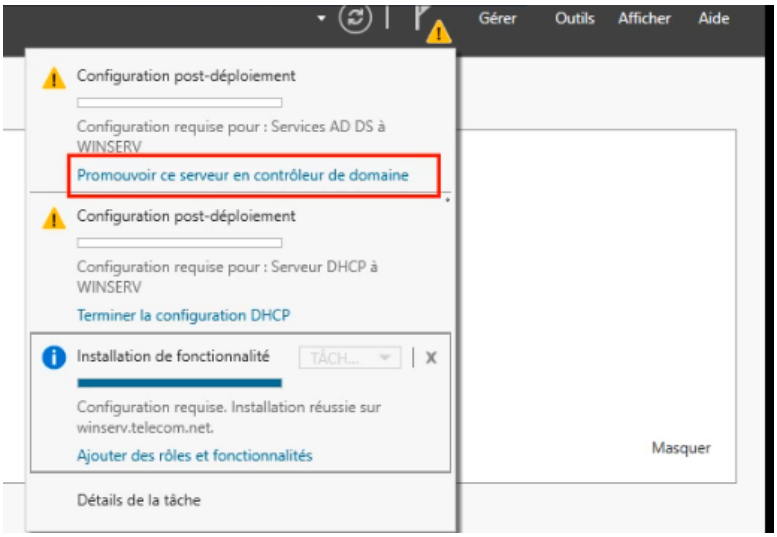
-Ouvrez le gestionnaire du serveur ajouter les rôles et fonctionnalité :


DÉMARRAGE RAPIDE
NOUVEAUTÉS
EN SAVOIR PLUS
Configurer ce serveur local
Ajouter des rôles et des fonctionnalités
Ajouter d'autres serveurs à gérer
Créer un groupe de serveurs
Connecter ce serveur aux services cloud
Rôles et groupes de serveurs
Rôles : 1 | Groupes de serveurs : 1 | Nombre total de serveurs : 1
Services de fichiers et de stockage
Facilité de gestion
Événements
Performances
Résultats BPA
Serveur local
Facilité de gestion
Événements
Services
Performances
Résultats BPA
05/08/2025 09:00
Assistant Ajout de rôles et de fonctionnalités
Sélectionner le serveur de destination
SERVEUR DE DESTINATION
winser.telecom.net
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.
Sélectionner un serveur du pool de serveurs
Sélectionner un disque dur virtuel
Pool de serveurs
Filtre :
Nom
Adresse IP
Système d'exploitation
winser.telecom.net
169.254.253.63
Microsoft Windows Server 2019 Standard
1 ordinateur(s) trouvé(s)
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.
< Précédent
Suivant >
Installer
Annuler

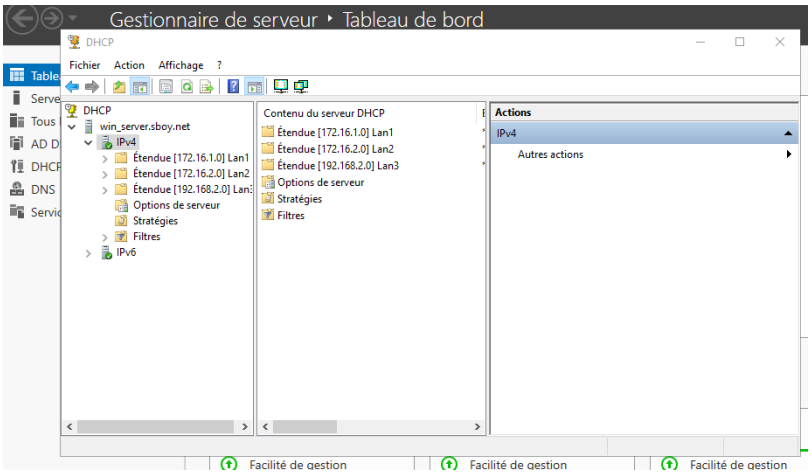
-installer d'abord le serveur DHCP et le Serveur AD DS en même temps (cliquer juste sur suivant et installer)


Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
winserv.telecom.net
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DHCP
AD DS
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Accès à distance
Attestation d'intégrité de l'appareil
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Service Guardian hôte
Services AD DS
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manage
Services Bureau à distance
Services d'activation en volume
Services d'impression et de numérisation de docu
Services de certificats Active Directory
Services de déploiement Windows
Services de fédération Active Directory (AD FS)
Services de fichiers et de stockage (1 sur 12 install
Services de stratégie et d'accès réseau
Description
Les services de domaine Active Directory (AD DS) stockent des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.
< Précédent
Suivant >
Installer
Annuler

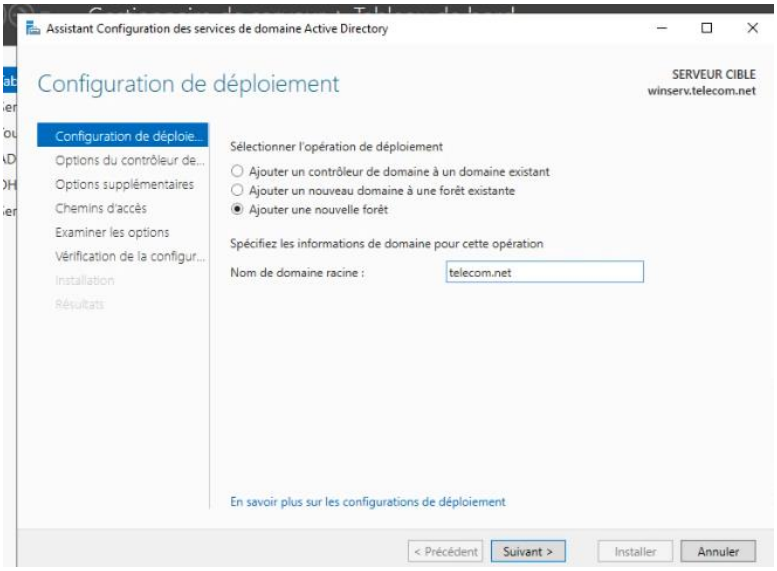
-Vous recevrez cette notification terminer la configuration DHCP et Promouvoir le Serveur AD DS en contrôleur de domaine (ce qui permettra d'installer automatique ont un serveur DNS):



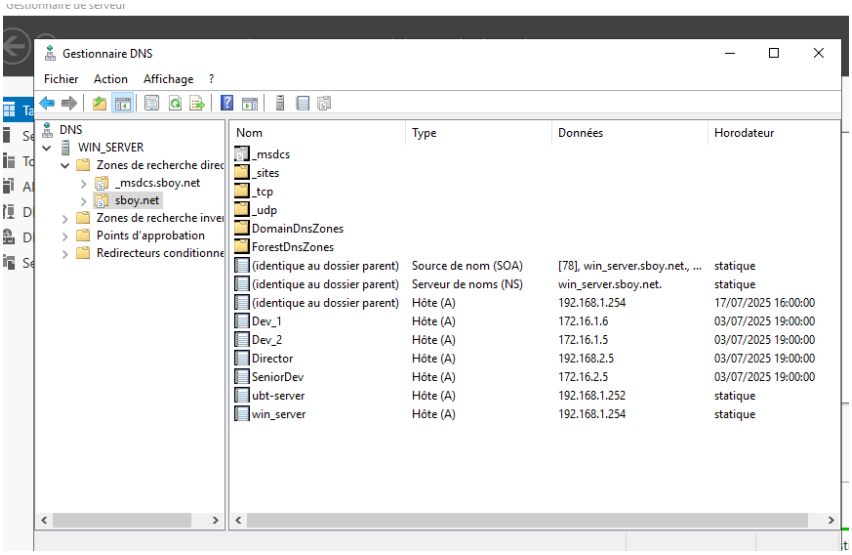
-Pour terminer les config DHCP, créez une nouvelle étendue pour chaque réseau de notre lab. avec la plage d'adresse souhaiter : (aller vérifier sur chaque host en effectuant un ping)



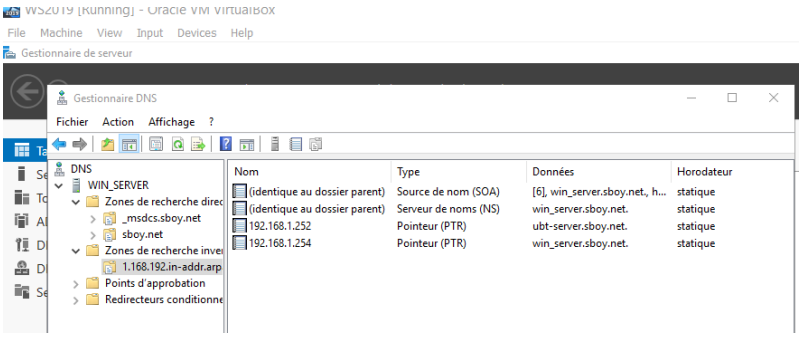
-Une fois fait, promouvoir AD DS en contrôleur de domaine ceci permettra d'installer automatiquement le DNS : (mettez un mot de passe en cliquer sur suivant, ne cocher rien d'autre



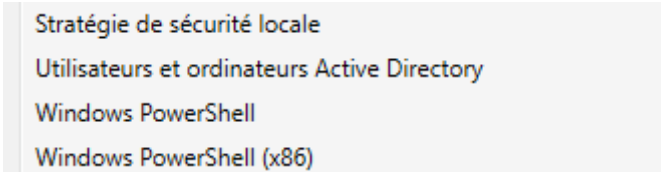
-Accéder au gestionnaire du DNS et ajouter les Hôtes avec adresse statique, ceux en DHCP seront ajouter automatiquement



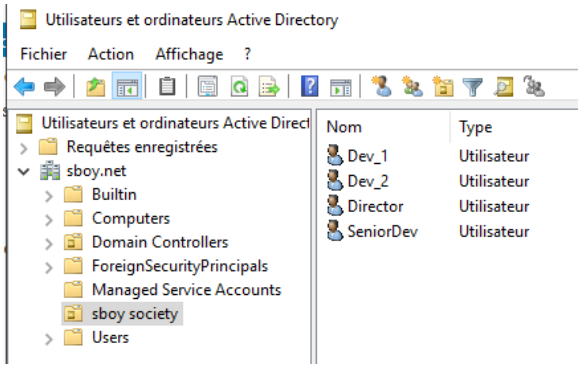
-N'oublier surtout pas de créer une zone de recherche inverser pour les 2 serveur :



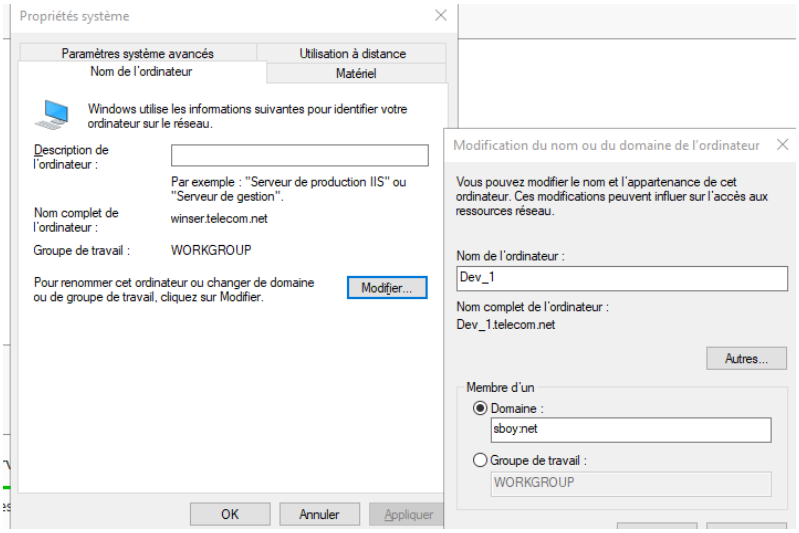
-Maintenant rendez-vous en haut à droite dans votre gestionnaire d'utilisateur et cliquer sur utilisateurs et ordinateurs active directory



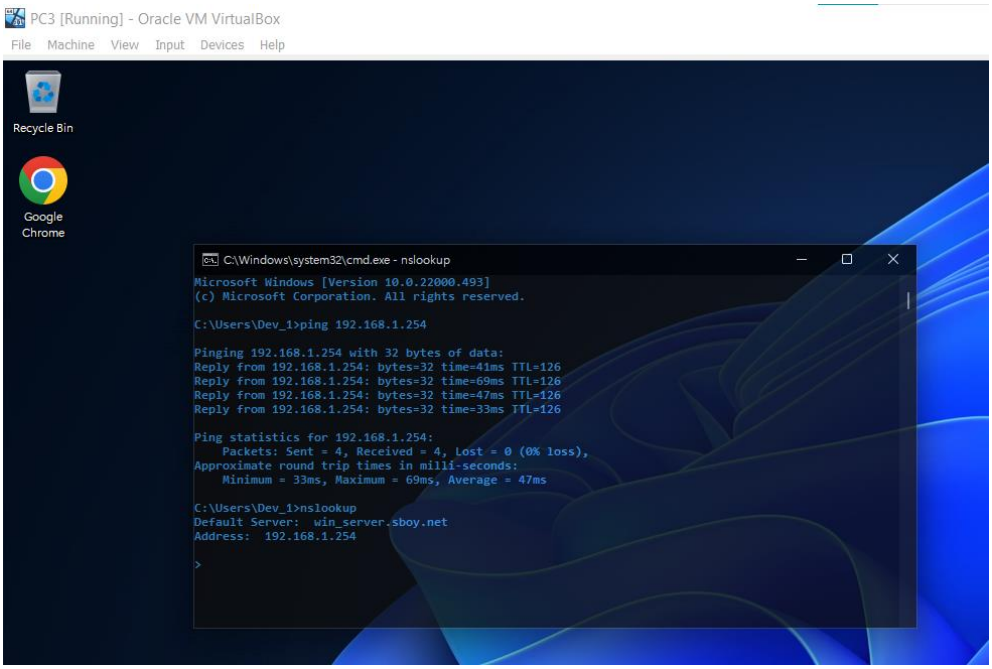
-Créez les différents utilisateurs de votre réseau :



-rendez vous sur chaque client, taper Windows + R (sydm.cpl) et insérer les dans le domaine et assigner chaque utilisateur a un PC selon la Topologie


Propriétés système
Paramètres système avancés
Utilisation à distance
Nom de l'ordinateur
Matériel
Windows utilise les informations suivantes pour identifier votre ordinateur sur le réseau.
Description de l'ordinateur :
Par exemple : "Serveur de production IIS" ou "Serveur de gestion".
Nom complet de l'ordinateur :
winser.telecom.net
Groupe de travail :
WORKGROUP
Pour renommer cet ordinateur ou changer de domaine ou de groupe de travail, cliquez sur Modifier.
Modifier...
OK
Annuler
Appliquer
Modification du nom ou du domaine de l'ordinateur
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.
Nom de l'ordinateur :
Dev_1
Nom complet de l'ordinateur :
Dev_1.telecom.net
Autres...
Membre d'un
Domaine :
sboy.net
Groupe de travail :
WORKGROUP

-une fois que c'est fait vous n'avez qu'a actualiser réseaux de vos hôtes Windows 11 et faire un Ping ou nslookup


PC3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Google Chrome
C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Dev_1>ping 192.168.1.254
Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=41ms TTL=126
Reply from 192.168.1.254: bytes=32 time=69ms TTL=126
Reply from 192.168.1.254: bytes=32 time=47ms TTL=126
Reply from 192.168.1.254: bytes=32 time=33ms TTL=126
Ping statistics for 192.168.1.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 33ms, Maximum = 69ms, Average = 47ms
C:\Users\Dev_1>nslookup
Default Server: win_server.sboy.net
Address: 192.168.1.254

5-Administration système Linux

Un serveur Ubuntu a été déployé (nom : `ubt-server-1`) dans le VLAN Serveurs (192.168.1.0/24), avec une IP statique définie à **192.168.1.252**.

- Version installée : Ubuntu Server 22.04 LTS
- Configuration minimal : 2 vCPU, 2 Go RAM, 20 Go disque
- Accès SSH activé pour l'administration distante
- Mises à jour appliquées via `apt update && apt upgrade`

-connecter bien avant tout votre serveur a internet en NAT et télécharger les paquets suivants ainsi que la procédure d'installation de Zabbix ci-dessous

Service	Commande
Nginx	apt install nginx
DHCP	apt install isc-dhcp-server
DNS	apt install bind9
TFTP	apt install tftpd-hpa
Samba	apt install samba
Zabbix Agent	apt install zabbix-agent
Zabbix Server	apt install zabbix-server-mysql` |
Nagios	apt install nagios3
FTP	apt install vsftpd
SSH	apt install openssh-server
UFW	apt install ufw
Fail2ban	apt install fail2ban

5.1 Installation de Zabbix

Pour vous permettre une installation étape par étape et je vous redirige vers le liens suivant :

https://youtu.be/nFulGCNc89A?si=R8ebBVr6A2snjcYv

Zabbix a été choisi comme outil principal de supervision pour ses fonctionnalités avancées, son interface moderne et sa compatibilité multi-OS.

Étapes d'installation : (vous trouverez toute les etapes sur le site officiel de Zabbix)

https://www.zabbix.com/fr/download

- Ajout du dépôt officiel Zabbix
- Installation de la base de données MySQL/MariaDB
- Installation de zabbix-server-mysql, zabbix-frontend-php, zabbix-agent
- Configuration du serveur et démarrage des services

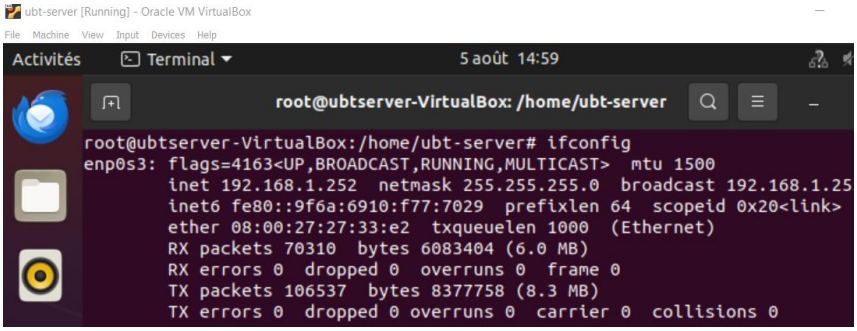
Accès :

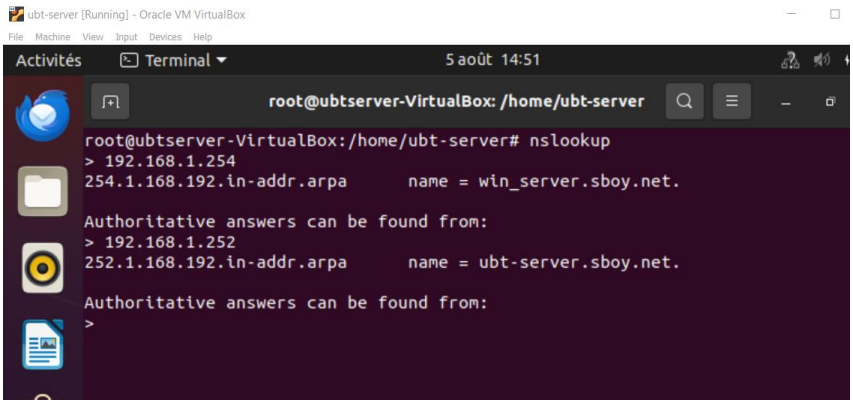
- Interface web : http://192.168.1.252/zabbix
- Utilisateur admin Zabbix créé pour la gestion

  Installer un agent zabbix sur votre serveur ou activer tout simplement le protocol snmpd sur votre serveur :

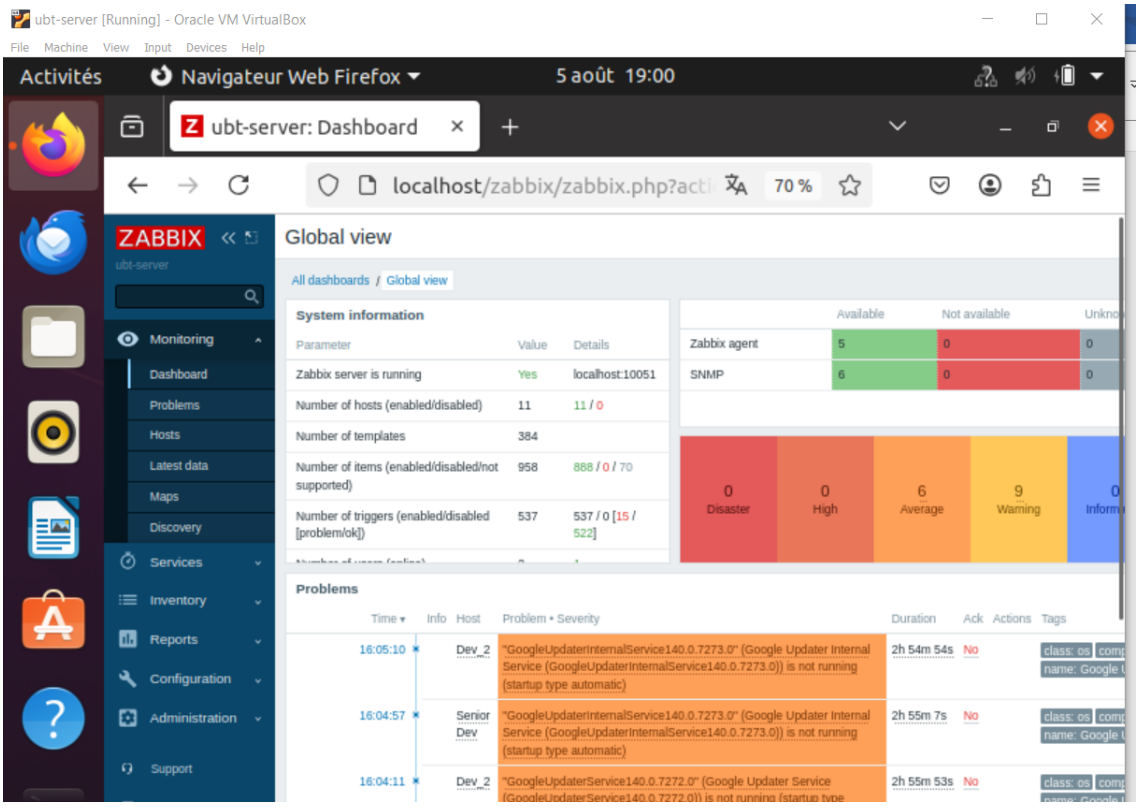
  https://youtu.be/D5uifMiVdbY?si=rjllJWKar86BSRIP

- Attribuer l'adresse 192.168.1.252 au serveur Ubuntu et mettez l'adresse du serveur Windows comme adresse DNS. Faite un Nslookup pour vérifier les config du nom de domaine


ubt-server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activités
Terminal
5 août 14:59
root@ubtserver-VirtualBox: /home/ubt-server
root@ubtserver-VirtualBox:/home/ubt-server# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.252 netmask 255.255.255.0 broadcast 192.168.1.25
inet6 fe80::9f6a:6910:f77:7029 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:27:33:e2 txqueuelen 1000 (Ethernet)
RX packets 70310 bytes 6083404 (6.0 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 106537 bytes 8377758 (8.3 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0



-Entrer dans le navigateur https://192.168.1.252./zabbix et connecter vous:



-Ajoutez les routeurs du reseaux a Zabbix. Pour ce faire il vous faudra activer le protocole snmp sur chaque port des Lan respectifs de chaque routeur :

############## SNMP CONFIG #############

R 1

#snmp-server community ROUTER ro

#snmp-server enable traps config

#snmp-server host 192.168.1.1 version 2c ROUTER

R 3

#snmp-server community ROUTER ro

#snmp-server enable traps config

#snmp-server host 192.168.2.1 version 2c ROUTER

R2

#snmp-server community ROUTER ro

#snmp-server enable traps config

#snmp-server host 172.16.1.1 version 2c ROUTER

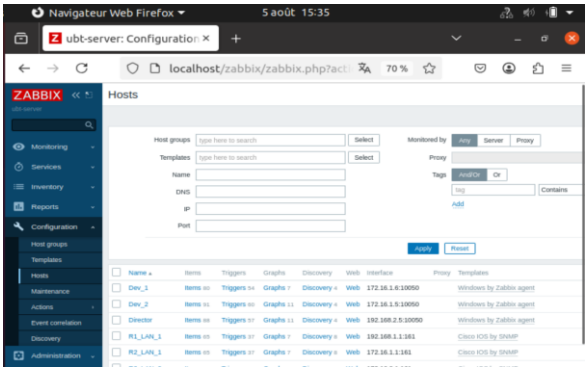
#snmp-server host 172.16.2.1 version 2c ROUTER

5.2. Supervision des postes clients

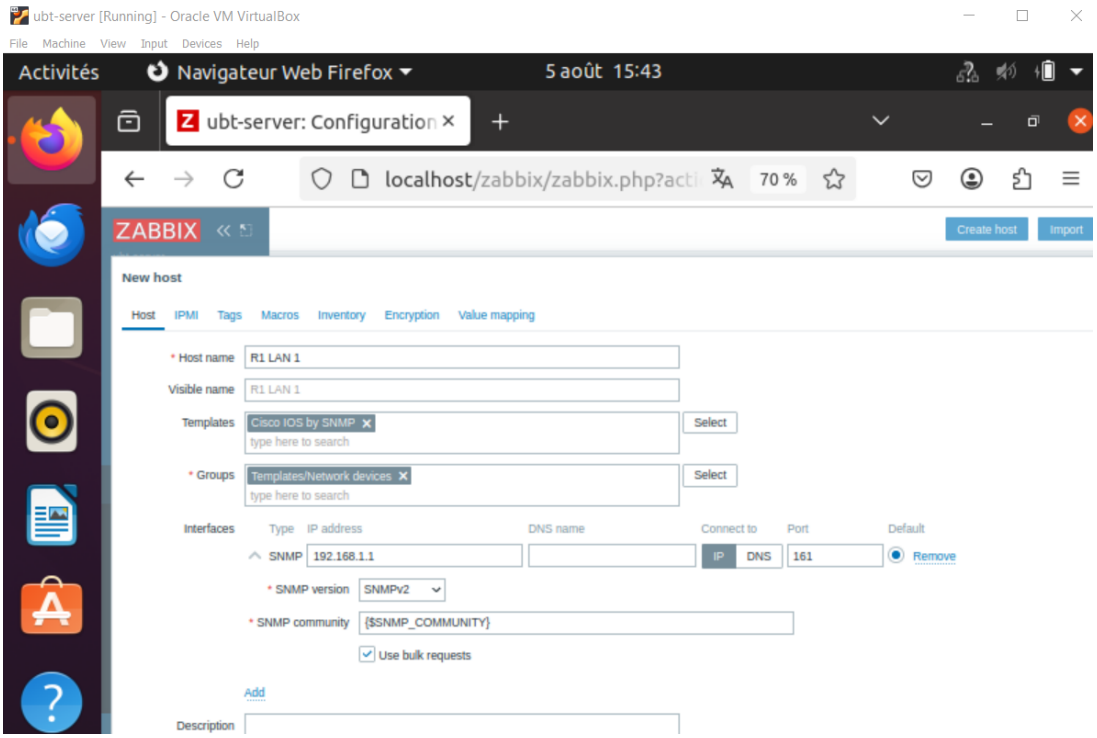
Zabbix Agent a été installé sur les postes cibles Linux et Windows.

- Ajout manuel ou via auto-Discovery
- Surveillance CPU, RAM, services critiques
- Alertes configurées pour la perte de connectivité, surcharge mémoire ou disque
- Possibilité d'étendre vers des métriques personnalisées (ping, ports, services réseau

-Ajouter les 3 routeur sur zabbix : (Via Protocol SNMP



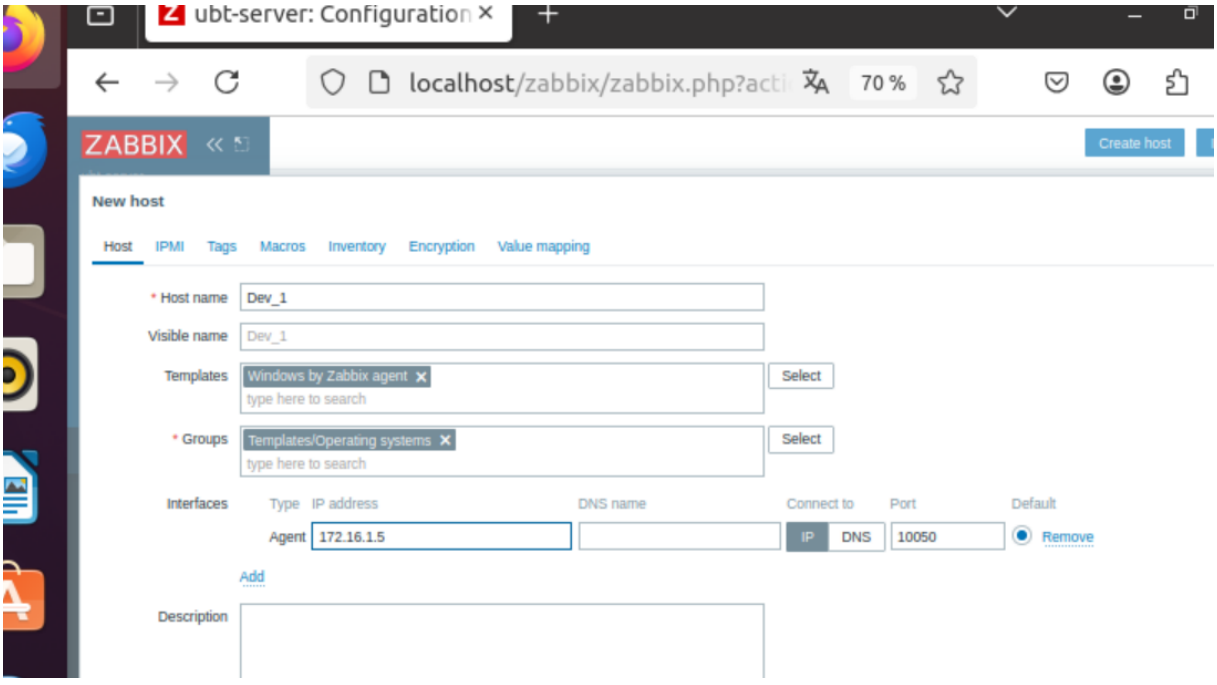
-clique en haut a droite sur creat host et placer les configurations suivantes :

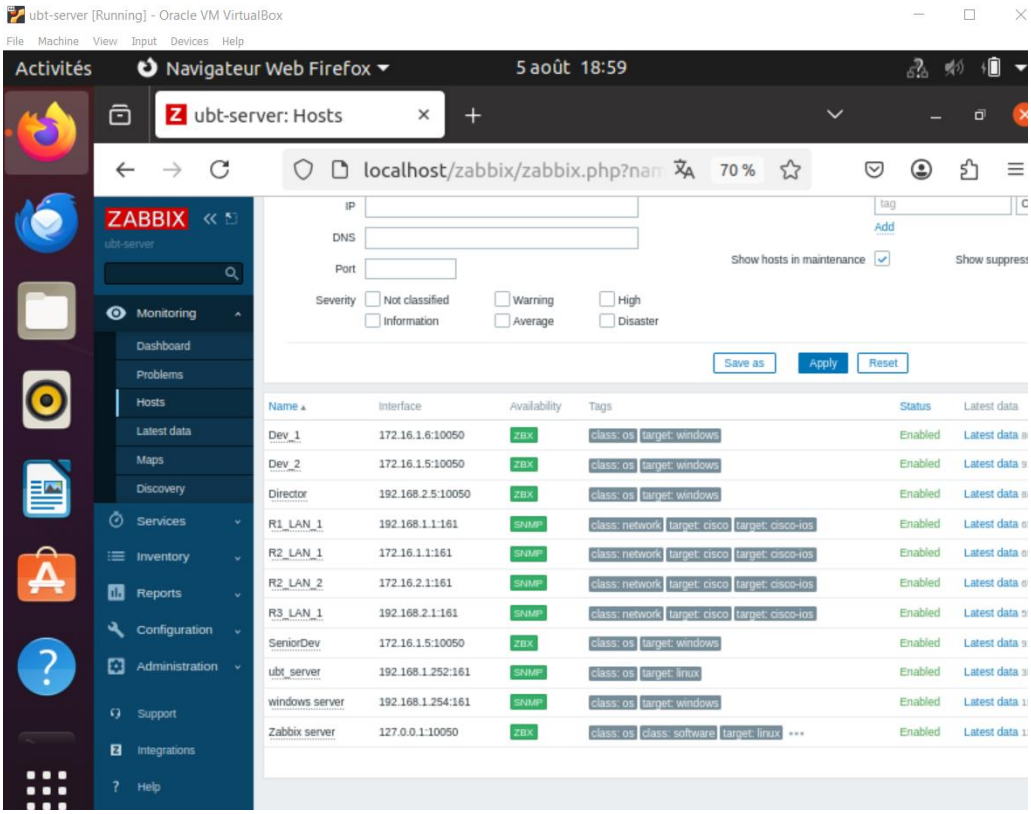


Faite de même pour les 3 autres routeurs.

-Ajouter les Machines Windows sur Zabbix via Zabbix agent : (Zabbix Discovery ou manuellement)

https://youtu.be/nFulGCNc89A?si=0ldABDpbiIIpMvz4

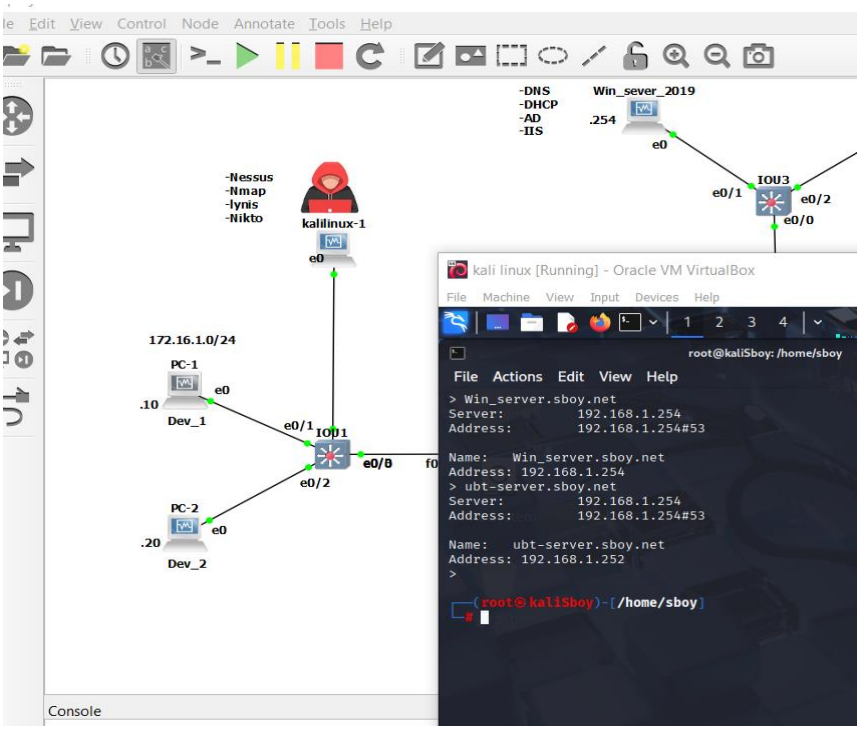




Une fois toute les machine de notre réseaux ajouter pourrai suivre leur fonctionnement leur évolution (CPU & RAM).

6. Sécurité offensive – Kali Linux

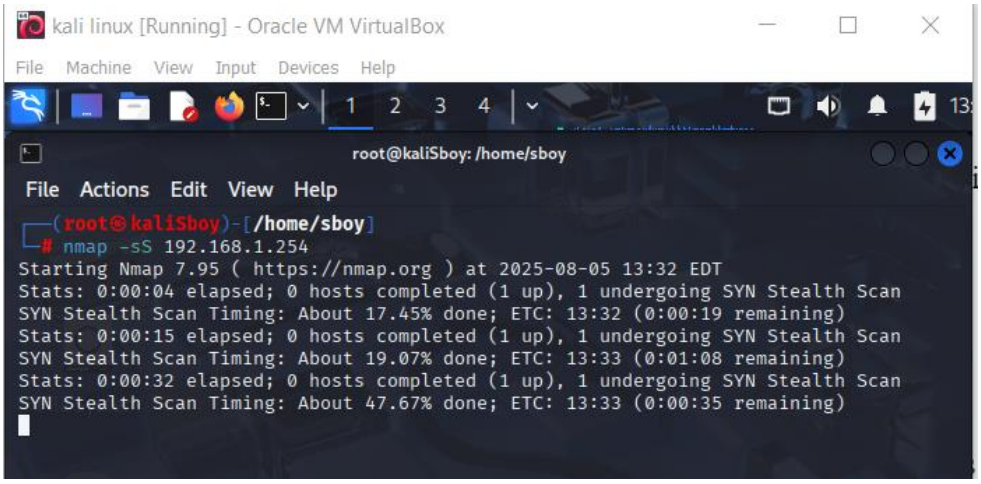
Le moment est venu d'intégrer notre OS de sécurité qui nous permettra d'effectuer des test de vulnérabilité en tant qu'auditeur interne

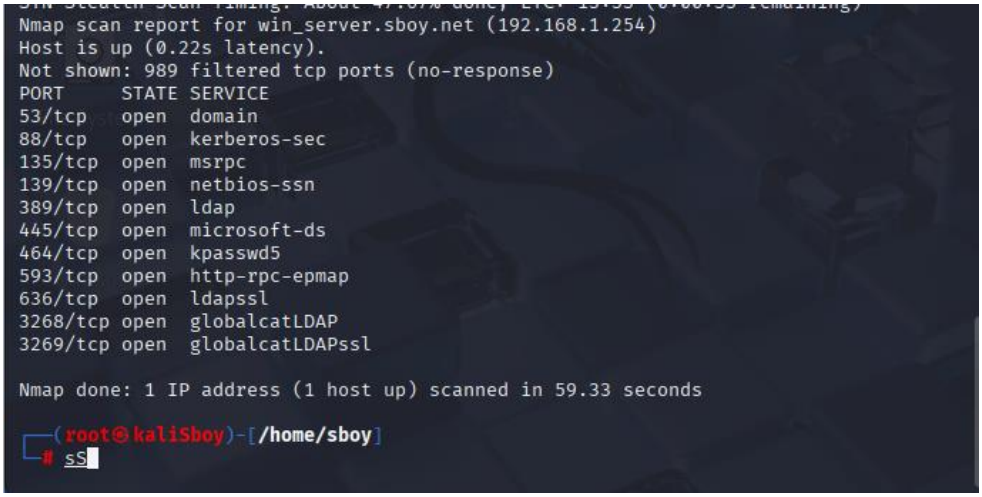


6.1. Scans de vulnérabilités internes

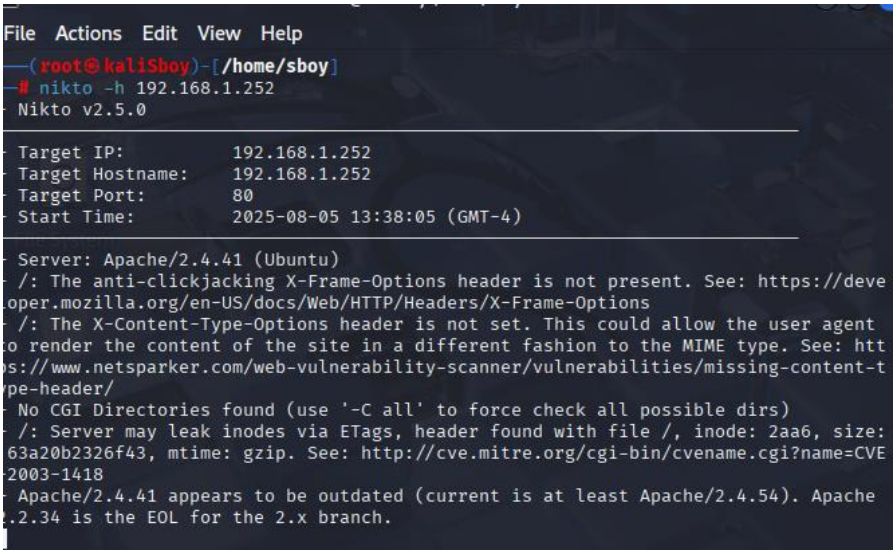
La distribution Kali Linux est intégrée au réseau pour simuler des audits de sécurité. Les outils principaux utilisés sont :

Nmap : scan de ports, découverte réseau

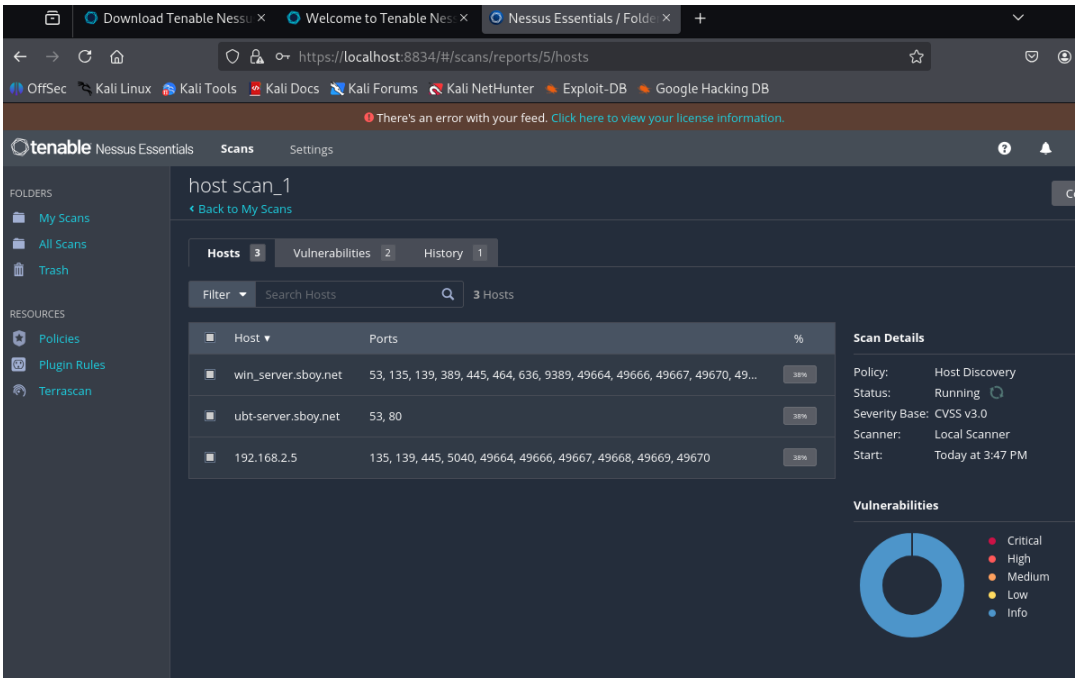

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kaliSboy: /home/sboy
File Actions Edit View Help
(root㉿kaliSboy)-[/home/sboy]
nmap -sS 192.168.1.254
Starting Nmap 7.95 (https://nmap.org) at 2025-08-05 13:32 EDT
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.45% done; ETC: 13:32 (0:00:19 remaining)
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.07% done; ETC: 13:33 (0:01:08 remaining)
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.67% done; ETC: 13:33 (0:00:35 remaining)



Nikto : scan de vulnérabilités web du serveur apache2 (192.168.1.252)


File Actions Edit View Help
(root㉿kaliSboy)-[/home/sboy]
nikto -h 192.168.1.252
- Nikto v2.5.0
- Target IP: 192.168.1.252
- Target Hostname: 192.168.1.252
- Target Port: 80
- Start Time: 2025-08-05 13:38:05 (GMT-4)
- Server: Apache/2.4.41 (Ubuntu)
- /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
- /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
- No CGI Directories found (use '-C all' to force check all possible dirs)
- /: Server may leak inodes via ETags, header found with file /, inode: 2aa6, size: 63a20b2326f43, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
- Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.

Nessus : scan de vulnérabilités à haut niveau avec rapports graphiques 192.168.1.252



7. Bonnes pratiques & documentation

Dans tout environnement professionnel ou de test, l'adoption de bonnes pratiques est cruciale pour garantir la stabilité, la sécurité et la traçabilité du système. Ce lab n'échappe pas à la règle.

7.1. Sauvegarde et snapshots

- **Snapshots réguliers** de toutes les VM (avant et après chaque configuration critique)
- Sauvegarde manuelle des fichiers de configuration (.conf, .cfg, etc.)
- Export des configurations routeurs Cisco via TFTP ou copie locale

7.2. Sécurisation des accès

- Comptes root désactivés en SSH distant (Linux)
- Comptes utilisateurs séparés par rôle (admin, dev, utilisateur)
- Authentification avec mot de passe fort + expiration périodique
- Firewall local configuré (UFW sur Ubuntu, règles ACL sur Cisco)

7.3. Nommage cohérent

- **Machines nommées** selon un schéma clair : PC3-1, WS2019-1, R2, ubt-server-1, etc.
- Interfaces réseau identifiées et commentées sur les routeurs
- VLAN et sous-réseaux nommés selon la fonction (LAN Dev, LAN Directeur, etc.)

7.4 Journalisation des actions

- Utilisation de script sous Linux pour enregistrer les sessions de configuration
- Notes techniques documentées au fur et à mesure
- Export des logs Windows via Event Viewer
- Centralisation des journaux prévue via rsyslog (non encore implémentée)

8. Axes d'amélioration

Le lab mis en place constitue déjà une base solide, mais des améliorations peuvent encore l'enrichir pour approcher une architecture réseau d'entreprise encore plus réaliste.

8.1. Intégration d'un firewall

- Ajout d'une VM **pfSense**, **Cisco ASA** ou pare-feu Linux avec iptables
- Contrôle avancé des flux inter-VLAN ou vers l'extérieur
- Analyse des logs pare-feu et détection d'anomalies
- Ajout d'un SIEM

8.2. Ajout de serveurs web vulnérables

- Intégration de VM telles que :
    - **DVWA** (Damn Vulnerable Web Application)
    - **Metasploitable 2 ou 3**
    - **OWASP Broken Web Apps**
- But : servir de cibles à des audits et attaques réalistes avec Kali

8.3. Redondance réseau et haute disponibilité

- Ajout de routeurs ou switches pour simuler la tolérance aux pannes
- Configuration de HSRP/VRRP ou de liens EtherChannel
- Tests de basculement de route et de services critiques

8.4. Suggestions de la communauté

« Rien n'est jamais parfait. Si vous avez des idées d'ajouts ou d'optimisations (ex. : nouveaux services, sécurité avancée, outils de détection), n'hésitez pas à contribuer à l'évolution du lab. »

Ce document a été conçu, rédigé et structuré par Koffivi Joel M. AMETEPE dans le cadre d'un projet personnel et pédagogique.Il est protégé au titre de la propriété intellectuelle et ne peut en aucun cas être copié, distribué ou présenté comme le travail d'un tiers sans accord explicite.